Defense Research Engineering Network (DREN) Service Agreement

15 January 2003

Defense Research Engineering Network Service Agreement (DSA)

1 Purpose

This Defense Research Engineering Network (DREN) Service Agreement (DSA) establishes the terms and agreements between the DREN Site Organization and the High Performance Computing (HPC) Modernization Program Office (HPCMPO) for use of the DREN. It documents the guidelines and procedures to be observed by the Site Organization. The DSA constitutes the "contract" between the Site Organization and the HPCMPO. The DSA is made up of five parts:

a. Site Organization concurrence letter (attachment 1)
b. Consent to monitor (attachment 3)
c. Network Diagram of the Site's DMZ and Local Area Networks (LANs) connected to SDP. If your LAN includes encryption device(s), do not show the equipment behind the encryption device(s).
d. Required security documentation (5.6.2)
e. Point of Contact (PoC) list (attachment 5)

The Site Organization and the DREN PoC must concur with all terms of this DSA, as a prerequisite to receiving and maintaining a DREN connection.

1.1 Concurrence – Concurrence is provided by submitting a signed Site Organization Concurrence Letter. See Attachment 1. It must be signed by the appropriate personnel for the Site Organization and by the DREN PoC. For contractor facilities, the DSA must additionally be signed by the DREN Sponsor Organization in order to certify that the contractor is required to meet the terms of this agreement and that such terms are within the scope of their contract.

2 Applicability

This DREN Service Agreement applies to all Organizations receiving DREN services.

3 Definitions

3.1 DREN Site – The location (Post, Camp, Base, Station, contractor facility, etc.) where the SDP will be installed and DREN Wide Area Networking (WAN) service will be delivered.
3.2 DREN Site Organization – The organization responsible for the DREN SDP. The Site Organization must have authority to make the commitments that are required in this DSA. The Site Organization must comply with all security requirements in the DREN Operating Guidelines (see 5.6) before a DREN connection will be provided.
3.3 DREN User Organization – The organization that has the requirement for DREN connectivity. In most cases this is the same as the Site Organization. However, at some Sites, the Site Organization will be another organization that controls the local network infrastructure for the DREN User Organization (for example, the Consolidated Network Communications Center (CNCC) for the Air Force or the Director of Information Management (DOIM) for the Army) as part of support for the DREN User Organization.
3.4 Service Delivery Point (SDP) – The physical location where the DREN WAN capability connects to the LANs present at the Site. Normally, an SDP will consist of one rack (or less) of Contractor-provided and installed equipment (ATM devices, routers, access termination equipment, security equipment, etc.) that connects to the DREN WAN capability.
3.5 DREN Point of Contact (PoC) – The Site Organization's appointed representative who has the responsibility to ensure that the terms of this DSA are met and that the User Organization's requirements, with respect to DREN connectivity, are met.

3.6 DREN Project Manager (DREN PM) – The individual appointed by the Director, HPCMP, with overall responsibility for all aspects of the DREN.
3.7 DREN Contract – The contract, DCA200-02-D-5003, is a follow-on to the DREN Inter-Site Services Contract (DISC), and was awarded on April 4, 2002 by DISA's Defense Information Technology Contracting Organization. It provides state-of-the-art WAN capability for HPCMP and DMSO User Organizations and HPCMP HPC Centers..
3.8 Contractor – WorldCom Communications, Inc is the contractor for the DREN Contract.
3.9 DREN Network Operations Center (DREN NOC) – The network operations center operated by the Contractor with overall responsibility for operation and management of the DREN WAN capability.
3.10 Secret DREN (SDREN) – A subset of the DREN Sites that exchange data classified at the DoD Secret level or above.
3.11 DREN Sponsor Organization – The DoD sponsoring agency/organization that supports connection by an academic or industrial contractor facility to DREN.

4 Documentation

This DSA contains the terms for using the DREN and delineates the DREN PoC responsibilities. Other relevant documentation includes:
- The DREN Contract
- The generic SDP Plan Template, particularly the General Site Data and Site Survey (sections 1 and 7)
- Site-specific SDP Plans.

5 DREN Operating Guidelines

5.1 Mission – The DREN's primary mission is to provide high capacity, high bandwidth, low latency low jitter connectivity for organizations with validated HPCMP project requirements. In addition the DREN supports 1) Department of Defense (DoD) science & technology (S&T) organizations, 2) DoD test and evaluation (T&E) organizations, 3) the Missile Defense Agency, 4) Defense Threat Reduction Agency, and 5) DoD modeling and simulation (M&S) (non-S&T and non-T&E) organizations.
5.2 Acceptable Use – The DREN PM, acting in support of the Director, HPCMP, and the Director, Defense Modeling and Simulation Office (DMSO), is the governing authority in making determinations concerning acceptable use of the DREN. Acceptable use is governed by DoD regulations, including DoD Regulation 5500.7, particularly paragraph 2-301, which says (among other things), "*Federal Government communication systems and equipment (including ... electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only*." DREN services are intended to support efforts within the communities listed in the Mission (above) by providing appropriate access to scarce HPCMP and DMSO resources. Additionally the DREN provides an infrastructure, which supports and fosters collaborative investigative efforts among DoD users, as well as among DoD efforts and related government and industrial organizations and academic institutions. Use of the DREN for other purposes is not acceptable.
5.2.1 Acceptable and encouraged uses of DREN resources include but are not limited to the following:
1. Communication with U.S. and foreign national citizens in connection with authorized activities to the extent permitted by regulatory guidance, as long as any network that the foreign national citizen employs for such communications provides reciprocal access to U.S. citizens.
2. Communication and exchange for professional development, to maintain currency, or to debate issues in a field or subfield of DoD-related research or engineering.

3. Communication between contractors and their subcontractors for the purpose of conducting business in support of an HPCMP or DMSO related activity.
4. Use for disciplinary-society, government-advisory, or standards activities related to the user's activities.
5. Use in applying for or administering grants or contracts for DoD supported research or instruction, but not for other fund raising or public relations activities.
6. Any other administrative communications or activities in direct support of other acceptable uses.
7. Announcements of new products or services for use in conjunction with HPCMP or DMSO related activities, *but not for-profit advertising of any kind*.
8. Any traffic originating from a network of another member agency of the Interagency Working Group on Information Technology Research and Development, if the traffic meets the acceptable use policy of that agency.
9. Communication incidental to otherwise acceptable use, except for illegal or specifically unacceptable use.

5.2.2 Unacceptable uses of DREN resources include but are not limited to the following:

10. Use to conduct for-profit activities, unless covered by the General Principle or as a specifically acceptable use.
11. Extensive use for private or personal business.
12. Use for the conduct of or to aid in the conduct of illegal or prohibited activities.
13. Use that is intended to interfere with or disrupt other users of DREN services, or equipment or networks accessible via the DREN. Disruptions include, but are not limited to, terrorist activities, distribution of unsolicited advertising, and propagation of computer worms or viruses.
14. Use to attempt unlawful or unauthorized access to computational, information, or communications devices and resources, as well as other equipment accessible via the DREN.
15. Transfer of information, in violation of applicable federal copyright laws and patents, federal export control laws and regulations, or DoD or Service/Agency security regulations and directives.

5.3 Management – Overall management and administration responsibility for the DREN lies with the DREN PM but requires a team effort. Close coordination between the HPCMPO (primarily the DREN PM) and the DREN PoCs is a critical success factor. The DREN PM is the responsible for:

(1) Enacting guidelines issued by the Director, HPCMP.
(2) Overall coordination, planning and liaison activities between the DREN community and the Contractor.

Site Organizations are responsible for obtaining any required technical assistance not specifically provided for in this document.

5.4 Funding – Unless otherwise agreed to, one years funding must be in place before any DREN connection can be ordered/ installed, either provided by the User Organization or by the HPCMPO in the presence of validated HPCMP project requirements. The DREN PM will provide funding particulars once he and the Site Organization have come to an agreement that a DREN connection should be installed.

5.5 Appointment of DREN PoC – The Site Organization will appoint a DREN PoC and at least one alternate POC who are responsible for all issues involving the DREN. Roles and responsibilities are further defined in section 7. At Government Site Organizations, the PoCs and alternates should be Government employees of the Site Organization. For all Site Organizations, government, academic or industrial contractor, or other non-government, the DREN PoCs and alternates must be employees with the authority to discharge the roles and responsibilities of section 7 and ensure that all requirements of this DSA are met. DREN PoCs and alternates must be readily available, including via electronic mail. The Site Organization must keep a current, accurate record of all

DREN PoCs and alternates which includes each person's name, address, telephone number, electronic mail address, etc., and must inform the DREN PM and DREN NOC of all changes. This may be accomplished by sending a letter or by sending electronic mail to the addressees in Attachment 2.

5.6 Security

5.6.1 DREN Requirements – The DREN digital data transfer services are commercial services that are Sensitive But Unclassified. **All Site Organizations must acknowledge the SBU nature of the DREN services and accept the attendant risks and implications for User Organization and data security.** The DREN Contract states:

(1) SECURITY SERVICE REQUIREMENT

The Contractor shall ensure availability, confidentiality, and integrity of the DREN components, support systems, and databases being maintained by the Contractor in support of DREN service. The Contractor shall provide protection to ensure the availability of provided network service to authorized users and the confidentiality of customer profile and traffic. DREN shall satisfy security requirements described in: DoD Directive 5200.28, DoDI 5200.40. Security mechanisms will provide sufficient levels of assurance for vendor and Government security administrators, but will be as transparent as possible to the DREN user community. DREN security service requirements specified in this document are described in the following sections: Access Control, Identification and Authentication, Confidentiality and Integrity, Physical Security, and Personnel Security.

(2) CONFIDENTIALITY AND INTEGRITY

The security mechanisms implemented by the Contractor shall provide confidentiality and integrity for all DREN user information. DREN user information shall not be disclosed or modified by any entity other than the intended recipient or personnel who have a job-related requirement for access to the information as per DoDD 5200.28 3/21/1988 SECURITY REQUIREMENTS FOR AUTOMATED INFORMATION SYSTEMS (AISS) section E2.1.29. Need-to-Know. The Contractor shall ensure confidentiality and integrity of DREN information through the use of DREN owned and registered ASN. Interfaces with the DREN shall be limited to Government approved NAP, MAE, and other private peering points. The integrity and security of the Contractor provided network shall be maintained at all times, including but not limited to the following events: failure of network management center, failure of individual channels or ports, failure of trunks, and failure of lines. The Contractor provided network shall:

a) Protect sensitive management/control data transmitted between network management facilities and network components from unauthorized disclosure during transmission;
b) Have the ability to detect modification of sensitive management/control data transmitted between network management facilities and network components during transmission; and
c) All Information Assurance (IA) solutions used by the Contractor shall be evaluated using the Common Criteria Evaluation and Validation Scheme based on the National Information Assurance Program (NIAP) process as it may apply to the DREN requirements.

(3) CERTIFICATION AND ACCREDITATION SUPPORT

The Contractor shall support the C&A process as delineated in the approved SSAA. The Contractor shall, at the discretion of Government, provide for access to Contractor facilities and personnel involved in system design, engineering, operations, and security. The Contractor shall support the Government's accreditation of the DREN in accordance with DoDI 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP). The Contractor shall perform the following service to support security certification and accreditation in accordance with DoD and Government directives:

a) Provide access to test-bed configurations that will allow security testing;
b) Assist in the testing process;
c) Provide copies of component design specifications, user manuals and results of completed security tests or vulnerability assessments;
d) Resolve problems, faults or issues that result from the testing process;
e) Develop a security operations plan defining all aspects of DREN security procedure; and
f) Develop and update Standard Operating Procedures.

The Contractor shall resolve, within 180 days, problems resulting from the security certification and accreditation process including vulnerability assessments. Resolution shall include Contractor provided assistance with security problem reports, technical investigations, testing, and regression testing procedures for correcting security defects identified during security testing activity.

5.6.2 DREN Site Accreditation – DoD Directive 8500.1, Information Assurance (IA), 24 October 2002, establishes the authority for the Defense Information Systems Agency (DISA) security accreditation process. DISA Instruction 630-230-19, Information Systems Security Program, July 1996, requires that all information systems regardless of classification or sensitivity will achieve compliance with the minimum-security requirements stated therein. **All DREN Sites must be accredited in accordance with this regulation, at the SBU system high mode, following the DITSCAP.** Responsibility for the security accreditation resides with the Site Organization Designated Approving Authority (DAA).

5.6.2.1 Evidence of security certification is required as part of the accreditation process. Each Site Organization may use its own security certification team or request security certification service from the DISA. For some Sites (for example, those collocated with HPCMP HPC Centers) the HPCMPO will require a Comprehensive Security Assessment (CSA) before a final authority to connect is issued. The DREN PM will address this issue as part of the connection process.

5.6.2.2 If the security accreditation is not yet in place, the Site Organization DAA may issue an Interim Authority to Operate (IATO) for the Site. A copy of the IATO must be submitted to the DREN PM, along with a description of the tasks remaining in order to achieve full accreditation and a timeline for their implementation must be included as supporting documentation. The DREN PM will review the documentation and may at his/her discretion proceed with DREN connection process or withhold connection until the accreditation is complete.

5.6.2.3 All DREN Sites must submit to Security Test and Evaluations (ST&E) and/or CSAs if required by HPCMPO. ST&Es and CSAs evaluate the security posture of the Site. Currently only Sites collocated with HPCMP HPC Centers and SDREN Sites have this requirement, but other DREN Sites may be inspected in the future.

5.6.2.4 The DREN PM will not authorize final connection to establish DREN connection until the HPCMPO has received and reviewed adequate security documentation. In all cases this includes letter(s) of accreditation for all equipment, including LANs, connected to the SDP, and any IATO issued by the Site Organization DAA. For Sites collocated with an HPC Center, this includes AIS plan(s) for the HPCMP assets installed in the HPC Center.

5.6.2.5 If classified information is to be transported using the DREN, the Site Organization must provide for protection of the information independent of the DREN. Site Organization accreditation of the Site must assert that measures are in place to provide assurance that the independent protection is adequately provided. For classified information, an MOA with any organization with whom data is exchanged must be provided. For SDREN use, the SDREN Connection Approval Process (CAP) including the SDREN MOA must be followed. Responsibility for the security accreditation resides with the Site Organization DAA.

5.6.3 Monitoring – In accordance with the requirements of Chairman Joint Chief of Staff Instruction (CJCSI) 6510.01B, Defensive Information Operations Implementation, 22 August 1997, with change 1, 26 August 1998, and guidelines issued by the Director, HPCMP, the DREN is monitored

for security purposes. All Site Organizations must sign Consent to Monitor Statement as part of the DSA. See Attachment 3.

5.6.4 DREN Security Requirements – All Sites are required to meet existing and future DREN security requirements. All DoD networks, including the DREN, are tightening and improving security in response to increased threats. DREN security requirements will generally be contained in the "DREN Operating Guidelines" section of the most current DSA but, for actions requiring prompt action, may also be communicated via electronic mail or phone from the DoD HPC CERT or HPCMPO. *Specifically the DREN PoC must ensure that the Site is positioned to respond immediately to emerging security requirements. These could include the requirement to limit service or temporarily disconnect from the DREN.*

5.6.4.1 Sites collocated with HPCMP HPC Centers are monitored by Network Intrusion Detection Systems (NIDSs). Site Organizations for these Sites must assist in management of the NIDS and respond to all incidents and events reported by the HPCMP Computer Emergency Response Team (CERT).

5.6.4.2 In the future, some or all Site Organizations *may be required to purchase, install, maintain and/or operate security equipment as directed by the DREN PM* (For example, intrusion detection systems, firewalls, security routers, encryption devices, etc.).

5.6.5 Service/Agency Security Requirements – Site Organizations must meet all security requirements imposed by their respective Service or Agency (S/A). If the requirements of the mission for which the DREN connection is being obtained are incompatible with S/A requirements, an agreement with the S/A must be reached before a DREN connection will be approved.

6 DREN Services and Requirements

6.1 Types of Services/Connections – The DREN can provide connectivity to (nearly) any location within the 50 United States, including Alaska and Hawaii, and to OCONUS locations. Types of Service (e.g., IP or ATM, interface types, etc.) are listed in Attachment 4.

6.2 Management – DREN service management is performed by the Contractor and includes routine services including IP route management, ATM PVC/PVP setup and SVC signaling, service coordination (24 hours per day via the DREN NOC), and certain automated monitoring. DREN services provided by the Contractor include operation and maintenance of the SDP at the Site and DREN WAN infrastructure engineering.

6.3 Training – The Contractor shall provide instructional services (e.g., formal, informal, self-paced, automated, remotely accessed) to Government-designated personnel (including DREN end users, Site operators, DREN PoCs, and Site managers) for the purposes of fully understanding/utilizing the services provided under this Contract.

As a minimum, the instructional services shall address how to:

a) Report DREN-related problems and follow-up on previously reported problems;
b) Utilize the SDP analysis and testing capability;
c) Request SDP routine operational services; and
d) Perform SDP setup for connectivity to the WAN.

If instruction is provided at a Government facility, the Government will provide access to and use of classroom space, equipped with lighting, seating, and writing surfaces for students receiving such training.

6.4 SDP Plans – Following receipt of an order for new or modified SDP service, the Contractor will provide an SDP Plan as the first deliverable in accordance with the DREN Contract provisions. The DISA Contracting Office and the DREN PM will coordinate the review and approval of the plan with the participation of the Site Organization and the HPCMPO as applicable. The approved SDP Plan will provide the specific tasks and schedule to be executed by the Contractor in accomplishing the ordered installation or modification action.

6.5 SDP Equipment – According to the terms of the DREN Contract, the Contractor or its designated sub-contractor is required to provide all the equipment necessary to implement the service for the SDP, including the provision of all cable/fiber to the SDP and the equipment cabinet. There is no Government furnished equipment permitted under the DREN Contract.

6.5.1 The Site Organization must provide power, air conditioning, physical security and sufficient floor space available to accommodate the SDP cabinet. (Approximately 2 feet wide, 3 feet deep, 6 feet high.) Also see "Equipment Accountability", paragraph 7.5 below.

6.6 SDP Relocation – Periodically there may be a requirement to relocate communications and automated data processing equipment to accommodate changes and expansions at the local level. Due to the nature of DREN services, it is imperative that the Site Organization follows these procedures for SDP relocation.

(1) If SDP relocation is required, contact the DREN PM who must approve and transfer the request to the DISA Contracting Officer. The Contractor will accomplish the actual relocation, including all site survey work, site preparation, relocation, and service restoration. If the DREN PM determines that the Site Organization is responsible for funding, those funds must be in place before the relocation will be authorized.

(2) *At no time is the Site Organization authorized to move Contractor equipment at the Site without DREN PM approval*.

6.7 Logistics Support – In general, the Contractor is responsible for all logistics associated with services under the DREN Contract. Spare equipment is generally kept and maintained by Contractor personnel.

(1) Technical assistance may be required at a Site. Such assistance will be provided by consultation with the DREN NOC personnel, see paragraph 7.4.

(2) There is no equipment acquired by the Government as a result of its using the DREN Contract; however, the DREN PoC may have custodial care responsibilities for Contractor equipment at the Site, see paragraph 7.5.

6.8 SDP Failure Reporting – In general, anyone who notices that the SDP is not operating properly may report the failure to the DREN NOC personnel. The person making the report must identify herself/himself, identify the organization and the geographical location of the Site, describe the perceived problem and stand ready to be contacted by DREN NOC personnel for verification of the operational status of the SDP. The DREN NOC is responsible for opening a trouble ticket upon notification, making a determination as to whether the SDP is out of service, and if so, make arrangements for its repair.

6.8.1 According to the DREN Contract, the Contractor shall resolve/correct all reported troubles. The Contractor shall take all necessary actions to resolve troubles, including arrangements for access to the SDPs. The Contractor shall manage trouble resolution for all trouble calls by:

a) Providing real time, on-line status of all open trouble ticket status to HPCMPO;
b) Developing a plan for correcting problems that is agreeable to all involved parties; and
c) Correcting the problems in accordance with accepted plans.

The Contractor shall provide trouble resolution capabilities to meet the following requirements delineated in Table 6.8.1.

TABLE 6.8.1
Required Response and Repair Times

Category	Time Interval
Time to answer trouble report by human operator	60 seconds
Time to respond to a trouble report	30 minutes
Time to clear trouble report w/o field visit	2 hours
Time to on-site visit by field technician (if required):	
• Key SDP sites designated by HPCMPO*	4 hours
• Other sites	5 hours
Time to repair with on-site field visit:	
• Key SDP sites designated by HPCMPO*	5 hours
• Other sites	8 hours
• Public peering sites may require on-site technician support to provide shorter response times	

* Key sites are defined as those collocated with HPC Centers and those that perform gateway functions with other networks.

6.9 SDP Routine Operational Services – The DREN PoC and any identified alternate(s) are the only persons authorized to request Routine Operational Services (ROS) from the DREN NOC for the local SDP. The DREN PoC and alternate(s) must be registered with the DREN NOC and the DREN PM, as described in paragraph 7.3, before any ROS requests can be accepted.

6.9.1 The person making an ROS request must be authenticated by the DREN NOC personnel using the following process:
(1) The requester calls the DREN NOC, states the desired ROS, and hangs up.
(2) The DREN NOC personnel, using a pre-established telephone number will call back the individual.
(3) The individual will provide a previously registered identifying code (four characters) that will be matched by the DREN NOC personnel against a database. If a match exists, the ROS will be accepted, if not, the ROS will be denied.

6.9.2 Examples of ROS that may be requested include: adding or removing IP routes (when applicable), accessing SDP interface and routing data residing in the Contractor's equipment, and accessing Management Information Base (MIB) selections.

7 DREN PoC Roles and Responsibilities

The DREN PoC has overall responsibility for the actions and tasks listed below. Designated alternates may fill-in at the request or in the absence of the DREN PoC. However, the DREN PoC retains overall responsibility to ensure task/action completion.

7.1 DREN Guidelines – The DREN PoC has primary responsibility for enforcement of all DREN Guidelines (see section 5 above).

7.2 Problem Resolution – The DREN PoC is the primary response agent for all failure and troubleshooting activities and is responsible for coordination with the on-site technical support staff to assure problems with the local communications infrastructure have, to the extent possible, been eliminated prior to reporting the failure to the DREN NOC.

7.2.1 The DREN PoC must coordinate with local installation infrastructure authorities as applicable to ensure that DREN-related matters are brought to the attention of the proper local officials when their participation is a procedural requirement for problem resolution.

7.3 Registration to Request SDP Routine Operational Services – The DREN PoC and any identified alternate(s) are the only persons authorized to request ROS from the DREN NOC for the local SDP. The DREN PoC and alternate(s) must be registered with the DREN NOC and the DREN PM before any ROS requests can be accepted. Registration is accomplished separately by each individual sending their name, organization, phone number and a four digit identifying code (e.g., last four numbers of the SSN) to the DREN NOC and the DREN PM via electronic mail.

7.4 On-site Technical Support Responsibilities – The DREN PoC must provide or arrange for on-site technical support to the DREN NOC in the following areas:

7.4.1 Coordinate, at the Site, the physical site preparation and the installation and activation of the SDP, and access circuit equipment. This coordination includes interactions with the DREN PM, the Contractor or its designated sub-contractors, local telephone personnel, and Service/Agency Operation and Maintenance (O&M) or Engineering and Installation (E&I) activities. (Contractor personnel will install and configure any Contractor equipment used to provide SDP services.)

7.4.2 Arrange for connectivity between the SDP and the User Organization's LANs.

7.4.3 Provide or arrange for operational assistance under the telephonic instruction of DREN NOC personnel.

7.4.4 Coordinate and monitor scheduled and unscheduled corrective maintenance, and allow for scheduled preventive maintenance as directed by DREN NOC personnel. The DREN PoC must also coordinate authorized outages with the respective User Organization and the DREN NOC.

7.5 Equipment Accountability – The DREN PoC is responsible for care and safekeeping of all installed Site equipment and equipment shipped to the Site for future installation. The Site equipment remains the property of the Contractor although it may be entered in the Site Organization's property book/equipment records for custodial purposes depending on Site Organization policies.

7.5.1 The DREN PoC may be requested to provide or arrange for temporary storage of some SDP parts, assemblies, and materials. These items are expected to be relatively small, e.g. cable assemblies, modems, etc. Typically, this material will need to be retained for only a few days.

7.6 Site Access Control and Security

7.6.1 The DREN PoC regulates access to the Site. The DREN PM will provide the DREN PoC an initial roster of Contractor personnel who are authorized access to SDP equipment. The DREN PoC should add names to this roster, as required by the DREN PM, and maintain a copy of the current roster of personnel authorized to access the Site.

7.6.2 The DREN PoC must ensure that no SDP equipment is moved, interfered with, or tamper with, and that no maintenance, other than external cleaning, is performed unless directed by DREN NOC personnel.

7.6.3 The DREN PoC shall implement Site physical security procedures as specified in applicable DoD and Service directives. Each SDP Plan will reflect the specific security requirements for a given Site.

7.7 General Administration and Coordination – The DREN PoC must:

7.7.1 Maintain up-to-date documentation including that issued by DREN PM and the Contractor. This documentation will include a copy of the current SDP Plan to be delivered to the DREN PoC during SDP activation.

7.7.2 Notify the office of the DREN PM of any situation, or any configuration changes to Site equipment, which may impact DREN operations, including planned or unplanned outages.

7.7.3 Serve as focal point for SDP operations. The DREN PoC must maintain close contact with all points-of-contact (i.e., User Organization PoCs, DREN NOC, local phone service personnel, etc.).

7.7.4 Maintain a list of telephone numbers, to support both liaison and local site support functions. This will include as a minimum, the DREN NOC, the point-of-contact for directly-connected equipment (routers, ATM switches, etc.) at that Site, and other telephone numbers such as those of the servicing telephone company, the local technical control, the local communications Operations & Maintenance (O&M) unit representative, and Contractor personnel responsible for equipment maintenance.

7.8 SDP Site Survey Assistance – The Contractor conducts Site surveys. These surveys require some support on the part of the Site Organization. This support may represent the first contact on the part of the DREN PoC with the various parties involved with set-up, test, and operations of the SDP. The DREN PoC should coordinate local assistance, as required, to successfully complete the Site survey.

7.8.1 Prior to the Site survey, the DREN PoC will arrange for conference room space to be used by the survey team. The DREN PoC will also ensure that all User Organizations affected by the SDP installation and operation, or having requirements for the Site attend the meeting about the Site survey. At a minimum, this includes the Site hosting organization (typically the Site Organization) and local telecommunications personnel.

7.9 Review of SDP Plans – When requested by the DREN PM, the DREN PoC will coordinate a Site Organization review of the Contractor-submitted SDP Plan to verify that local requirements, as obtained during the Site survey, are met. The results of this review must be communicated to the DREN PM in coordination with additional related SDP Plan reviews.

7.10 SDP Testing and Acceptance

7.10.1 The DREN PoC must witness Site-specific SDP Acceptance Testing conducted by the Contractor. This testing will be conducted when the SDP is initially installed, after a modification to the SDP, and after the SDP has been restored to operational condition following a failure. DREN NOC personnel will notify the DREN PoC of the schedule for each test.

7.10.2 The DREN PoC must become thoroughly familiar with the SDP operation and be able to exercise the Analysis and Testing capabilities built into the SDP. These capabilities will aid the DREN NOC in problem and fault isolation and in performance measurement and validation.

7.10.3 The DREN PoC should be able, after training or with assistance from DREN NOC personnel, to recognize what is considered to be normal operating conditions for the SDP equipment. The DREN PoC should report any abnormal conditions to the DREN NOC.

7.10.4 The DREN PoC may be required to participate in a Collective SDP test, which is a test of the Contractor's supporting infrastructure, if the Site is part of a collective test set.

7.10.5 The results of all observed testing will be communicated to the DISC PM in coordination with additional related SDP testing observations.

7.11 SDP and Circuit Installation Assistance

7.11.1 The DREN PoC monitors the work of Government personnel, O&M command, the Contractor, and other commercial vendors supporting the Site. The DREN PoC will notify the DREN PM via telephone or electronic mail whenever Government personnel or Contractor work performance problems are observed or when the DREN PoC suggests improvements to the Site. The following minimum tasks should be completed by Contractor personnel during SDP installation and prior to acceptance of the completed work:

(1) SDP equipment and access circuit installed according to the SDP Plan.
(2) SDP is operational as determined by testing with the DREN NOC.
(3) All equipment (racks, drawers, patch panels, cables, modems, etc.) is properly labeled.
(4) All technical documentation is on hand, correct, and coordinated with the DREN NOC.

7.11.2 The DREN PoC, in conjunction with vendors and/or Government Engineering and Installation (E&I) teams, will assist with:

(1) Identification of space to house SDP equipment.
(2) Circuit installations between the commercial vendor and the SDP.

(3) Identification of appropriate cross-connect points, circuit-wiring pairs required to complete an access circuit order.
(4) Circuit implementation coordinators, S/A E&I activities, and commercial telephone company installation or maintenance personnel by coordinating the assignment of cable pairs or channels on local carrier systems for tail circuits as requested.

7.11.3 When requested by the DREN PM or Contractor personnel, the DREN PoC will provide Site status on SDP installations in process.

8 Renewal of Service Agreement

This DSA must be renewed every three years, at a minimum. It must also be renewed 1) whenever the DREN PoC appointment changes (to ensure his/her acceptance of the responsibilities herein) or 2) upon request of the DREN PM (in the case of major changes in DREN guidelines or DREN Contract requirements). Renewal is accomplished by resubmitting the DREN Site Organization Concurrence Letter as described in paragraph 1.1.

Attachment 1

DREN SITE ORGANIZATION CONCURRENCE LETTER

STATEMENT OF AGREEMENT

1. Acknowledgment of Terms and Conditions

We acknowledge and understand the contents of the DREN Service Agreement and agree to comply with the DREN Operating Guidelines and to the roles and responsibilities contained therein for the DREN PoC.

2. Acknowledgment of unclassified and non-secure service

We acknowledge and understand that the DREN services are Sensitive But Unclassified (SBU) with attendant risks. We acknowledge that data protection is provided by best commercial practices against unauthorized access and sabotage, etc. while transiting the DREN WAN service provider's commercial infrastructure.

DREN PoC:

Signature _____ *Date* _____

Name _____ *Ident. Code* _____

Organization _____

Site Organization Commander/Director:

Signature _____ *Date* _____

Name _____

Organization _____

Title _____

DREN Sponsor Organization (only if an academic or industrial contractor facility):

Signature _____ *Date* _____

Name _____

Organization _____

Please complete and return this page to the, DREN PM / Suite 510; 1010 North Glebe Road; Arlington, Virginia 22201. DREN points of contact include Rodger Johnson (703) 812-8205 E-Mail: rjohnson@hpcmo.hpc.mil or Joe Molnar (703) 812-8205 E-Mail: molnar@hpcmo.hpc.mil.. The DREN PM fax number is (703) 812-9701.

DREN Sponsor Organization (for contractor facilities only) certifies that the contractor is required to meet the terms of this agreement and that such terms are within the scope of their contract.

Attachment 2

DREN Program Manager and DREN Contract Point of Contact Information

DREN Program Manager

DREN Program Manager / Rodger Johnson
1010 North Glebe Rd, Suite 510
Arlington, VA 22201-4795
Coml.: 703-812-8205, Fax: 703-812-9701
E-mail: rjohnson@hpcmo.hpc.mil

Deputy DREN Program Manager

Deputy DREN Program Manager / Alan Welday
1010 North Glebe Rd, Suite 510
Arlington, VA 22201-4795
Coml.: 703-812-8205, Fax: 703-812-9701
E-mail: awelday@hpcmo.hpc.mil

DREN Security Action Officer

DREN Security Action Officer / Joseph Molnar
High Performance Computing Modernization Office
1010 Glebe Road, Suite 510
Arlington, VA 22201-4795
Coml.: 703-812-8205, Fax: 703-812-9701
E-mail: molnar@hpcmo.hpc.mil

DREN Operations Manager

DREN Operations Manager / John Samios
1010 North Glebe Rd, Suite 510
Arlington, VA 22201-4795
Coml.: 703-812-8205, Fax: 703-812-9701
E-mail: jsamios@hpcmo.hpc.mil

DREN NOC

Coml.: 1-866-NOC-DREN (1-866-662-3736)
E-mail: dren-noc@hpcmo.hpc.mil.

Attachment 3

Consent to Monitor Statement
[This statement may be placed on organizational letterhead and formatted in accordance with organizational requirements. However, the content of the body must not be changed.]

MEMORANDUM FOR HIGH PERFORMANCE COMPUTING MODERNIZATION PROGRAM OFFICE

SUBJECT: CONSENT TO MONITOR FOR DREN

In accordance with the requirements of Chairman Joint Chief of Staff Instruction (CJCSI) 6510.01B, Defensive Information Operations Implementation, 22 August 1997, with change 1, 26 August 1998, and Defense Research Engineering Network (DREN) Operating Guidelines, we acknowledge that the DREN program manager, or their designated representative, will conduct periodic monitoring of the DREN. We acknowledge and consent to initial and periodic assessments of all connected systems and networks to determine the security features in place to protect against unauthorized access or attack. We accept the responsibility to notify all users, who access the DREN through our connection to the DREN, of these monitoring and assessment requirements.

<Site Organization DAA or Commander Signature>

<Site OrganizationDAA or Commander Signature Block>

Attachment 4

One SDP may have multiple physical interfaces, but they cannot exceed the aggregate SDP transfer rate.

DREN CONTRACT CLIN ORDERING OPTIONS	Interface Standard	Physical Interfaces
0100 USER SDP INTERFACE		
Service Type A IP Packet-Based		
0100AA	Fast Ethernet	100BaseT
0100AB	Fast Ethernet	100BaseF
0100AC	Gigabit Ethernet	1000Base-TX
0100AD	Gigabit Ethernet	1000Base-SX
0100AE	Gigabit Ethernet	1000BaseLX
0100AF	10-Gigabit Ethernet	10GBaseSX
0100AG	10-Gigabit Ethernet	10GBaseLX
0100AH	ATM (IP over ATM)	OC-3c Single Mode
0100AI	ATM (IP over ATM)	OC-3c Multi-Mode
0100AJ	ATM (IP over ATM)	OC-12c Single Mode
0100AK	ATM (IP over ATM)	OC-12c Multi-Mode
Service Type B ATM Cell-based		
0100AL	ATM	OC-3c Single Mode
0100AM	ATM	OC-3c Multi-Mode
0100AN	ATM	OC-12c Single Mode
0100AO	ATM	OC-12c Multi-Mode
0100AP	To be defined	To be defined

Note: ATM cells will not be transported as IP for a Service Type B SDP.

DREN CONTRACT CLIN WAN ACCESS ORDERING OPTIONS	Peak/Sustained SDP Transfer Rate	Aggregate SDP Transfer Rate
0101 – DREN Site		
0101AB	36.0/22.5 Mbps	45 Mbps (DS-3)
0101AC	124.0/77.5 Mbps	155.5 Mbps (OC-3c)
0101AD	497.6/311.0 Mbps	622 Mbps (OC-12c)
0101AE	995.2/622.0 Mbps	1244 Mbps (OC-24c)
0101AF	1990.4/1244.0 Mbps	2488 Mbps (OC-48c)
0101AG	7952.0/4970.0 Mbps	9940 Mbps (OC-192c)
0101AH	31808.0/19880.0 Mbps	39760 Mbps (OC-768c)

The Peak SDP Transfer rate is 80% of the aggregate SDP Transfer rate, and the Sustained SDP Transfer rate is 50% of the aggregate SDP Transfer rate.

Service Type C (Lightwave) is also defined on the DREN Contract, but is not available at this time.

Attachment 5

PRIMARY DREN POC:

NAME: _____
ADDRESS: _____
_____
_____
PHONE: _____
FAX: _____
DSN: _____
E-MAIL: _____

ALTERNATE DREN POC:

NAME: _____
ADDRESS: _____
_____
_____
PHONE: _____
FAX: _____
DSN: _____
E-MAIL: _____

SITE ORGANIZATION DESIGNATED APPROVAL AUTHORITY:

NAME: _____
ADDRESS: _____
_____
_____
PHONE: _____
FAX: _____
DSN: _____
E-MAIL: _____

SITE SECURITY MANAGER:

NAME: _____
ADDRESS: _____
_____
_____
PHONE: _____
FAX: _____
DSN: _____
E-MAIL: _____